CLAIMS

1. An information processing method for generating a hierarchical tree which is applied to processing for supplying cipher texts decryptable only by certain selected equipment except excluded (revoked) equipment, by applying a Broadcast Encryption scheme based on a hierarchical tree configuration, the information processing method characterized by comprising:

a one-way tree generating step of generating a one-way tree in which node-corresponding values are set to respective nodes, the node-corresponding values being set such that a node-corresponding value NV_a corresponding to each of the nodes constituting the hierarchical tree is calculable by application of a function f based on a node-corresponding value NV_b and a node-added variable $salt_b$ set so as to correspond to at least one lower-rank node;

a node key calculating step of calculating node keys NK corresponding to the respective nodes constituting the one-way tree, by application of a function Hc using the node-corresponding values NV corresponding to the respective nodes as inputs; and

an information-for-supply determining step of selecting a minimum node-corresponding value and node-added variables required to calculate node-corresponding values included in a path from a receiver-corresponding node to a root as a highest-rank node, as information to be supplied to a receiver corresponding to a terminal node of the one-way tree.

2. The information processing method according to Claim 1,

characterized in that:

the one-way tree generating step generates the one-way tree having a setting in which a node-corresponding value for a higher-rank node is calculable by encrypting processing (forward computation) to which a Rabin cryptography based on a node-corresponding value for a lower-rank node is applied, and in which the node-corresponding value for the lower-rank node is calculable by decrypting processing (inverse computation) to which a Rabin cryptography based on the node-corresponding value for the higher-rank node is applied.

3. The information processing method according to Claim 1, characterized by further comprising:

a cipher text generating step of generating cipher texts by executing encrypting processing by selectively applying the node keys set so as to correspond to the respective nodes of the hierarchical tree.

4. The information processing method according to Claim 1, characterized in that:

the one-way tree generating step generates the one-way tree in which, in a hierarchical tree having a binary tree configuration with a number N of terminal nodes, node-corresponding values NV_l ($l = 2, 3, \cdots, 2N-1$) for respective nodes l to which node numbers l are given from a higher-rank node in a breadth first order in the binary tree satisfy a relationship of the following expression

[Math 1]

$$NV_{\lfloor l/2 \rfloor} = (NV_l^{\,2} + H(l \,\|\, salt_l)) \bmod M$$

where M is a product of two large primes, and H is a mapping function for outputting an element of Z_M.

5. The information processing method according to Claim 4, characterized in that:

the one-way tree generating step includes, in a hierarchical tree having a binary tree configuration with a number N of terminal nodes, using, as inputs, a number of leaves as the number of node terminals: N, and a size of a modulus M: |M|,

a step 1: Determine two large primes of a size |M|/2, and calculate a product M thereof;

a step 2: Determine the mapping function for outputting an element of Z_M: H;

a step 3: Randomly select a node-corresponding value NV_1 for a root node being a highest-rank node of the binary tree as a value such that $NV_1 \in Z^*_M$;

a step 4: Perform the following processing a, b while incrementing l by 1 from 2 to 2N-1 using l as a counter

a. Find a minimum positive integer $salt_l$ such that tmp_l is a quadratic residue modulo M, in the following expression

[Math 2]

$$temp_l = (NV_{\lfloor l/2 \rfloor} - H(l \| salt_l)) \bmod M$$

b. Find $tmp_l^{1/2} \bmod M$, and determine any of four solutions as a node-corresponding value NV_l for a node l; and

a step 5: Output

2N-1 |M|-bit numbers (node-corresponding values): NV_1, NV_2, ⋯, NV_{2N-1}, and

2N-2 numbers (node-added variables): $salt_2$, $salt_3$, ⋯, $salt_{2N-1}$,
and set them as the node-corresponding values and the node-added variables for the respective nodes l (l = 1 through 2N-1) of the binary tree.

6. The information processing method according to Claim 1, characterized in that:

the node key calculating step is a step of calculating node keys NK by application of a function Hc using node-corresponding values NV corresponding to the respective nodes as inputs, wherein the function Hc is a hash function for mapping a node-corresponding value NV into data of a bitlength corresponding to a size of a node key.

7. The information processing method according to Claim 1, characterized in that:

the one-way tree generating step generates the one-way tree in which, in a hierarchical tree having a binary tree configuration with a number N of terminal nodes, node-corresponding values NV_l (l = 2, 3, ⋯, 2N-1) for respective nodes l to which node numbers l are given from a higher-rank node in a breadth first order in the binary tree satisfy a relationship of the following expression

[Math 3]

$$NV_{\lfloor l/2 \rfloor} = (NV_l^{\,2} \oplus H^{salt_l}(l)) \bmod M$$

where H is a function for mapping an input of any size into a size |M| of a product M of the said two large primes, and H^{saltl} (l) represents a value obtained by applying the function H to l as many as $salt_l$ times.

8. The information processing method according to Claim 7, characterized in that:

the one-way tree generating step includes, in a hierarchical tree having a binary tree configuration with a number N of terminal nodes, using, as inputs, a number of leaves as the number of node terminals: N, a size of a modulus M: $|M|$, and a mapping function H with an $|M|$-bit output,

a step 1: Determine two large primes of a size $|M|/2$, and calculate a product M thereof;

a step 2: Randomly select a node-corresponding value NV_1 for a root node being a highest-rank node of the binary tree as a value such that $NV_1 \in Z^*_M$;

a step 3: Perform the following processing a, b while incrementing l by 1 from 2 to 2N-1 using l as a counter

a. Find a minimum positive integer $salt_l$ such that tmp_l is a quadratic residue modulo M, in the following expression

[Math 4]

$$temp_l = (NV_{\lfloor l/2 \rfloor} \oplus H^{salt_l}(l)) \bmod M$$

b. Find $tmp_l^{1/2}$ mod M, and determine any of four solutions as a node-corresponding value NV_l for a node l; and

a step 4: Output

2N-1 $|M|$-bit numbers (node-corresponding values): NV_1, NV_2, …, NV_{2N-1}, and

2N-2 numbers (node-added variables): $salt_2$, $salt_3$, …, $salt_{2N-1}$,

and set them as the node-corresponding values and the node-added variables for the respective nodes l (l = 1 through 2N-1) of the binary tree.

9. An information processing method for generating a hierarchical tree applied to processing for supplying cipher texts decryptable only by certain selected equipment, using a Broadcast Encryption scheme based on a hierarchical tree configuration, the information processing method characterized by comprising:

a one-way tree generating step of generating a one-way tree in which node-corresponding values are set to respective nodes, the node-corresponding values being set such that a node-corresponding value NV_a corresponding to each of the nodes constituting the hierarchical tree is calculable by application of a function f based on a node-corresponding value NV_b and a node-added variable $salt_b$ set so as to correspond to at least one lower-rank node;

an intermediate label generating step of generating intermediate labels which are intermediate labels (IL) set as values from which values of labels corresponding to some selected special subsets, among labels (LABEL) respectively corresponding to subsets set on the basis of a SD (Subset Difference) scheme to which the hierarchical tree is applied, are calculable by computational processing;

a label generating step of generating the labels corresponding to the special subsets by computational processing based on the intermediate labels, and further generating labels not corresponding to the special subsets by a computation based on the generated labels; and

a labels-for-supply determining step of determining labels for supply to a receiver corresponding to a terminal node of the hierarchical tree, and selecting

the special subset-noncorresponding labels not corresponding to the special subsets, and

a node-corresponding value as a minimum intermediate label and node-added variables required to calculate a node-corresponding value for any node included in a path from a receiver-corresponding node to a root as a highest-rank node, as information for supply to the receiver corresponding to the terminal node of the one-way tree, and

wherein the one-way tree generating step generates the one-way tree in which, in a hierarchical tree having a binary tree configuration with a number N of terminal nodes, node-corresponding values NV_l (l = 2, 3, ⋯, 2N-1) for respective nodes l to which node numbers l are given from a higher-rank node of a binary tree in a breadth first order in the binary tree satisfy a relationship of the following expression

[Math 5]

$$NV_{\lfloor l/2 \rfloor} = (NV_l^{\,2} \oplus H^{salt_l}(l)) \bmod M$$

where H is a function for mapping an input of any size into a size |M| of a product M of the said two large primes, and H^{saltl} (l) represents a value obtained by applying the function H to l as many as $salt_l$ times.

10. The information processing method according to Claim 9, characterized in that:

the one-way tree generating step includes, in the hierarchical tree having the binary tree configuration with the number N of terminal nodes, using, as inputs, a number of leaves as the number of node terminals: N, a size of a modulus M: |M|, and a mapping function H with an |M|-bit output, a step 1: Determine two large primes of a size $|M|/2$, and calculate a product M thereof;

a step 2: Randomly select a node-corresponding value NV_1 for the root node being the highest-rank node of the binary tree as a value such that $NV_1 \in Z^*_M$;

a step 3: Perform the following processing a, b while incrementing l by 1 from 2 to 2N-1 using l as a counter

a. Find a minimum positive integer $salt_l$ such that tmp_l is a quadratic residue modulo M, in the following expression

[Math 6]

$$temp_l = (NV_{\lfloor l/2 \rfloor} \oplus H^{salt_l}(l)) \bmod M$$

b. Find $tmp_l^{1/2} \bmod M$, and determine any of four solutions as a node-corresponding value NV_l for a node l; and

a step 4: Output

2N-1 $|M|$-bit numbers (node-corresponding values): NV_1, NV_2, ⋯, NV_{2N-1}, and

2N-2 numbers (node-added variables): $salt_2$, $salt_3$, ⋯, $salt_{2N-1}$,

and set them as the node-corresponding values and the node-added variables for the respective nodes l (l = 1 through 2N-1) of the binary tree.

11. A decryption processing method for executing processing for decrypting cipher texts encrypted with node keys respectively corresponding to nodes constituting a hierarchical tree, by applying a Broadcast Encryption scheme based on a hierarchical tree configuration, the decryption processing method characterized by comprising:

a cipher text selecting step of selecting a cipher text to which a node key generable on the basis of a node-corresponding value NV and node-added variables salt held by a self apparatus, from the cipher texts;

a node key calculating step of calculating the node key applied to the cipher text on the basis of the node-corresponding value NV and the node-added variables salt held by the self apparatus; and

a decrypting step of executing processing for decrypting the cipher text on the basis of the calculated node key.

12. The decryption processing method according to Claim 11, characterized in that:

the cipher text selecting step is a step of finding, in a hierarchical tree in which respective nodes are given node numbers in a breadth first order with a root as a highest-rank node of the hierarchical tree numbered 1, a node number coinciding with any node number included in nodes in a path from a receiver to the root, among node numbers for node keys used for encryption.

13. The decryption processing method according to Claim 11, characterized in that:

the node key calculating step includes a step of calculating node-corresponding values in a path from a self node to a root being a highest-rank node, among node-corresponding values NV_l ($l = 2, 3, \cdots, 2N-1$) for respective nodes l to which node numbers l are given from a higher-rank node in a breadth first order in a binary tree, on the basis of the node-corresponding value NV and the node-added variables salt held by the self apparatus, by applying the following expression

[Math 7]

$$NV_{\lfloor l/2 \rfloor} = (NV_l^{\,2} + H(l \parallel salt_l)) \bmod M$$

where M is a product of two large primes, and H is a mapping function for outputting an element of Z_M.

14. The decryption processing method according to Claim 11, characterized in that:

the node key calculating step includes a step of calculating on the basis of the node-corresponding value held by the self apparatus, or node-corresponding values in a path from a self node to a root being a highest-rank node, and further on the basis of the following expression

NK = Hc (NV)

where NK is a node key; NV is a node-corresponding value; and Hc is a mapping function.

15. The decryption processing method according to Claim 11, characterized in that:

the node key calculating step includes a step of calculating node-corresponding values in a path from a self node to a root being a highest-rank node, among node-corresponding values NV_l (l = 2, 3, ⋯, 2N-1) for respective nodes l to which node numbers l are given from a higher-rank node in a breadth first order in a binary tree, on the basis of the node-corresponding value NV and the node-added variables salt held by the self apparatus, by applying the following expression

[Math 8]

$$NV_{\lfloor l/2 \rfloor} = (NV_l^{\,2} \oplus H^{salt_l}(l)) \bmod M$$

where H is a function for mapping an input of any size into a size |M| of a product M of the said two large primes, and H^{saltl} (l) represents a value obtained by applying the function H to l as many as $salt_l$ times.

16. A decryption processing method for executing processing for decrypting cipher texts encrypted with subset keys respectively corresponding to subsets set on the basis of a SD (Subset Difference) scheme which is a Broadcast Encryption scheme based on a hierarchical tree configuration, the decryption processing method characterized by comprising:

a cipher text selecting step of selecting a cipher text generated by applying a subset key derivable by pseudo-random number generating processing based on a label held by a self apparatus, or a label calculable on the basis of a node-corresponding value NV as an intermediate label, and node-added variables salt held by the self apparatus, from the cipher texts;

a label calculating step of calculating a label corresponding to a special subset by executing computational processing based on the node-corresponding value NV and the node-added variable salt, if the subset key to be applied to the cipher text is underivable by the pseudo-random number generating processing based on the label held;

a step of generating the subset key by the pseudo-random number generating processing based on the label held or the label calculated; and

a decrypting step of executing processing for decrypting the cipher text by applying the generated subset key, and

wherein the label calculating step includes a step of calculating node-corresponding values in a path from a self node to a root being a highest-rank node, among node-corresponding values NV_l (l = 2, 3, ⋯, 2N-1) for respective nodes l to which node numbers l are given from a higher-rank node in a breadth first order in a binary tree, on the basis of the node-corresponding value NV and the node-added variables salt held by the self apparatus, by applying the following expression

[Math 9]

$$NV_{\lfloor l/2 \rfloor} = (NV_l^2 \oplus H^{salt_l}(l)) \bmod M$$

where H is a function for mapping an input of any size into a size |M| of a product M of the said two large primes, and H^{saltl} (l) represents a value obtained by applying the function H to l as many as $salt_l$ times.

17. An information processing apparatus for generating a hierarchical tree which is applied to processing for supplying cipher texts decryptable only by certain selected equipment except excluded (revoked) equipment, by applying a Broadcast Encryption scheme based on a hierarchical tree configuration, the information processing apparatus characterized by comprising:

a one-way tree generating means for generating a one-way tree in which node-corresponding values are set to respective nodes, the node-corresponding values being set such that a node-corresponding value NV_a corresponding to each of the nodes constituting the hierarchical tree is calculable by application of a function f based on a node-corresponding value NV_b and a node-added variable $salt_b$ set so as to correspond to at least one lower-rank node;

a node key calculating means for calculating node keys NK corresponding to the respective nodes constituting the one-way tree, by application of a function Hc using the node-corresponding values NV corresponding to the nodes as inputs; and

an information-for-supply determining means for selecting a minimum node-corresponding value and node-added variables required to calculate node-corresponding values included in a path from a receiver-corresponding node to a root as a highest-rank node, as information to be supplied to a receiver corresponding to a terminal node of the one-way tree.

18. The information processing apparatus according to Claim 17, characterized in that:

the one-way tree generating means is configured to generate the one-way tree having a setting in which a node-corresponding value for a higher-rank node is calculable by encrypting processing (forward computation) to which a Rabin cryptography based on a node-corresponding value for a lower-rank node is applied, and in which the node-corresponding value for the lower-rank node is calculable by decrypting processing (inverse computation) to which a Rabin cryptography based on the node-corresponding value for the higher-rank node is applied.

19. The information processing apparatus according to Claim 17, characterized by further comprising:

a cipher text generating means for generating cipher texts by executing encrypting processing by selectively applying the node keys set so as to correspond to the respective nodes of the hierarchical tree.

20. The information processing apparatus according to Claim 17, characterized in that:

the one-way tree generating means is configured to generate the one-way tree in which, in a hierarchical tree having a binary tree configuration with a number N of terminal nodes, node-corresponding values NV_l ($l = 2, 3, \cdots, 2N-1$) for respective nodes l to which node numbers l are given from a higher-rank node in a breadth first order in the binary tree satisfy a relationship of the following expression

[Math 10]

$$NV_{\lfloor l/2 \rfloor} = (NV_l^{\,2} + H(l \,\|\, salt_l)) \bmod M$$

where M is a product of two large primes, and H is a mapping function for outputting an element of Z_M.

21. The information processing apparatus according to Claim 20, characterized in that:

the one-way tree generating means is configured to execute processing for generating the one-way tree by executing, in a hierarchical tree having a binary tree configuration with a number N of terminal nodes, using, as inputs, a number of leaves as the number of node terminals: N, and a size of a modulus M: |M|,

a step 1: Determine two large primes of a size |M|/2, and calculate a product M thereof;

a step 2: Determine the mapping function for outputting an element of Z_M: H;

a step 3: Randomly select a node-corresponding value NV_1 for a root node being a highest-rank node of the binary tree as a value such that $NV_1 \in Z^*_M$;

a step 4: Perform the following processing a, b while incrementing l by 1 from 2 to 2N-1 using l as a counter

a. Find a minimum positive integer $salt_l$ such that tmp_l is a quadratic residue modulo M, in the following expression

[Math 11]

$$temp_l = (NV_{\lfloor l/2 \rfloor} - H(l \| salt_l)) \bmod M$$

b. Find $tmp_l^{1/2}$ mod M, and determine any of four solutions as a node-corresponding value NV_l for a node l; and

a step 5: Output

2N-1 |M|-bit numbers (node-corresponding values): NV_1, NV_2, …, NV_{2N-1}, and

2N-2 numbers (node-added variables): $salt_2$, $salt_3$, …, $salt_{2N-1}$,

and set them as the node-corresponding values and the node-added variables for the respective nodes l (l = 1 through 2N-1) of the binary tree.

22. The information processing apparatus according to Claim 17, characterized in that:

the node key calculating means is configured to calculate node keys NK by application of a function Hc using node-corresponding values NV corresponding to the respective nodes as inputs, wherein the function Hc is a hash function for mapping a node-corresponding value NV into data of a bitlength corresponding to a size of a node key.

23. The information processing apparatus according to Claim 17, characterized in that:

the one-way tree generating means is configured to generate the one-way tree in which, in a hierarchical tree having a binary tree configuration with a number N of terminal nodes, node-corresponding values NV_l ($l = 2, 3, \cdots, 2N-1$) for respective nodes l to which node numbers l are given from a higher-rank node in a breadth first order in the binary tree satisfy a relationship of the following expression

[Math 12]

$$NV_{\lfloor l/2 \rfloor} = (NV_l^2 \oplus H^{salt_l}(l)) \bmod M$$

where H is a function for mapping an input of any size into a size |M| of a product M of the said two large primes, and H^{saltl} (l) represents a value obtained by applying the function H to l as many as $salt_l$ times.

24. The information processing apparatus according to Claim 23, characterized in that:

the one-way tree generating means is configured to generate the one-way tree by executing, in a hierarchical tree having a binary tree configuration with a number N of terminal nodes, using, as inputs, a number of leaves as the number of node terminals: N, a size of a modulus M: |M|, and a mapping function H with an |M|-bit output,

a step 1: Determine two large primes of a size |M|/2, and calculate a product M thereof;

a step 2: Randomly select a node-corresponding value NV_1 for a root node being a highest-rank node of the binary tree as a value such that $NV_1 \in Z^*_M$;

a step 3: Perform the following processing a, b while incrementing l by 1 from 2 to 2N-1 using l as a counter

a. Find a minimum positive integer salt$_l$ such that tmp$_l$ is a quadratic residue modulo M, in the following expression

[Math 13]

$$temp_l = (NV_{\lfloor l/2 \rfloor} \oplus H^{salt_l}(l)) \bmod M$$

b. Find tmp$_l^{1/2}$ mod M, and determine any of four solutions as a node-corresponding value NV$_l$ for a node l; and

a step 4: Output

2N-1 |M|-bit numbers (node-corresponding values): NV$_1$, NV$_2$, ⋯, NV$_{2N-1}$, and

2N-2 numbers (node-added variables): salt$_2$, salt$_3$, ⋯, salt$_{2N-1}$,

and set them as the node-corresponding values and the node-added variables for the respective nodes l (l = 1 through 2N-1) of the binary tree.

25. An information processing apparatus for generating a hierarchical tree applied to processing for supplying cipher texts decryptable only by certain selected equipment, using a Broadcast Encryption scheme based on a hierarchical tree configuration, the information processing apparatus characterized by comprising:

a one-way tree generating means for generating a one-way tree in which node-corresponding values are set to respective nodes, the node-corresponding values being set such that a node-corresponding value NV$_a$ corresponding to each of the nodes constituting the hierarchical tree is calculable by application of a function f based on a node-corresponding value NV_b and a node-added variable $salt_b$ set so as to correspond to at least one lower-rank node;

an intermediate label generating means for generating intermediate labels which are intermediate labels (IL) set as values from which values of labels corresponding to some selected special subsets, among labels (LABEL) respectively corresponding to subsets set on the basis of a SD (Subset Difference) scheme to which the hierarchical tree is applied, are calculable by computational processing;

a label generating means for generating the labels corresponding to the special subsets by computational processing based on the intermediate labels, and further generating labels not corresponding to the special subsets by a computation based on the generated labels; and

a labels-for-supply determining means for determining labels for supply to a receiver corresponding to a terminal node of the hierarchical tree, and selecting

the special subset-noncorresponding labels not corresponding to the special subsets, and

a node-corresponding value as a minimum intermediate label and node-added variables required to calculate a node-corresponding value for any node included in a path from a receiver-corresponding node to a root as a highest-rank node, as information for supply to the receiver corresponding to the terminal node of the one-way tree, and

wherein the one-way tree generating means is configured to generate the one-way tree, in which in a hierarchical tree having a binary tree configuration with a number N of terminal nodes, node-corresponding values NV_l ($l = 2, 3, \cdots, 2N-1$) for respective nodes l to which node numbers l are given from a higher-rank node of a binary tree in a breadth first order in the binary tree satisfy a relationship of the following expression

[Math 14]

$$NV_{\lfloor l/2 \rfloor} = (NV_{l}^{2} \oplus H^{salt_{l}}(l)) \bmod M$$

where H is a function for mapping an input of any size into a size |M| of a product M of the said two large primes, and H^{saltl} (l) represents a value obtained by applying the function H to l as many as $salt_l$ times.

26. The information processing apparatus according to Claim 25, characterized in that:

the one-way tree generating means is configured to generate the one-way tree by executing, in the hierarchical tree having the binary tree configuration with the number N of terminal nodes, using, as inputs, a number of leaves as the number of node terminals: N, a size of a modulus M: |M|, and a mapping function H with an |M|-bit output,

a step 1: Determine two large primes of a size |M|/2, and calculate a product M thereof;

a step 2: Randomly select a node-corresponding value NV_1 for the root node being the highest-rank node of the binary tree as a value such that $NV_1 \in Z^*_M$;

a step 3: Perform the following processing a, b while incrementing l by 1 from 2 to 2N-1 using l as a counter

a. Find a minimum positive integer $salt_l$ such that tmp_l is a quadratic residue modulo M, in the following expression

[Math 15]

$$temp_{l} = (NV_{\lfloor l/2 \rfloor} \oplus H^{salt_{l}}(l)) \bmod M$$

b. Find $tmp_1^{1/2}$ mod M, and determine any of four solutions as a node-corresponding value NV_1 for a node 1; and

a step 4: Output

2N-1 |M|-bit numbers (node-corresponding values): NV_1, NV_2, ···, NV_{2N-1}, and

2N-2 numbers (node-added variables): $salt_2$, $salt_3$, ···, $salt_{2N-1}$,

and set them as the node-corresponding values and the node-added variables for the respective nodes l (l = 1 through 2N-1) of the binary tree.

27. A decryption processing apparatus for executing processing for decrypting cipher texts encrypted with node keys respectively corresponding to nodes constituting a hierarchical tree, by applying a Broadcast Encryption scheme based on a hierarchical tree configuration, the decryption processing apparatus characterized by comprising:

a cipher text selecting means for selecting a cipher text to which a node key generable on the basis of node-corresponding values NV and node-added variables salt held by a self apparatus, from the cipher texts;

a node key calculating means for calculating the node key applied to the cipher text on the basis of the node-corresponding value NV and the node-added variables salt held by the self apparatus; and

a decrypting means for executing processing for decrypting the cipher text on the basis of the calculated node key.

28. The decryption processing apparatus according to Claim 27, characterized in that:

the cipher text selecting means is configured to find, in a hierarchical tree in which respective nodes are given node numbers in a breadth first order with a root as a highest-rank node of the hierarchical tree numbered 1, a node number coinciding with any node number included in nodes in a path from a receiver to the root, among node numbers for node keys used for encryption.

29. The decryption processing apparatus according to Claim 27, characterized in that

the node key calculating means

is configured to execute processing for calculating

node-corresponding values in a path from a self node to a root being a highest-rank node, among node-corresponding values NV_l (l = 2, 3, ⋯, 2N-1) for respective nodes l to which node numbers l are given from a higher-rank node in a breadth first order in a binary tree, on the basis of the node-corresponding value NV and the node-added variables salt held by the self apparatus, by applying the following expression

[Math 16]

$$NV_{\lfloor l/2 \rfloor} = (NV_{l}^{2} + H(l \parallel salt_{l})) \bmod M$$

where M is a product of two large primes, and H is a mapping function for outputting an element of Z_M.

30. The decryption processing apparatus according to Claim 27, characterized in that

the node key calculating means

is configured to execute processing for calculating on the basis of the node-corresponding value held by the self apparatus, or node-corresponding values in a path from a self node to a root being a highest-rank node, and further on the basis of the following expression

NK = Hc (NV)

where NK is a node key; NV is a node-corresponding value; and Hc is a mapping function.

31. The decryption processing apparatus according to Claim 11, characterized in that:

the node key calculating means is configured to execute processing for calculating node-corresponding values in a path from a self node to a root being a highest-rank node, among node-corresponding values NV_l (l = 2, 3, ⋯, 2N-1) for respective nodes l to which node numbers l are given from a higher-rank node in a breadth first order in a binary tree, on the basis of the node-corresponding value NV and the node-added variables salt held by the self apparatus, by applying the following expression

[Math 17]

$$NV_{\lfloor l/2 \rfloor} = (NV_l^2 \oplus H^{salt_l}(l)) \bmod M$$

where H is a function for mapping an input of any size into a size |M| of a product M of the said two large primes, and H^{saltl} (l) represents a value obtained by applying the function H to l as many as $salt_l$ times.

32. A decryption processing apparatus for executing processing for decrypting cipher texts encrypted with subset keys respectively corresponding to subsets set on the basis of a SD (Subset Difference) scheme which is a Broadcast Encryption scheme based on a hierarchical tree configuration,

the decryption processing apparatus characterized by comprising:

a cipher text selecting means for selecting a cipher text generated by applying a subset key derivable by pseudo-random number generating processing based on a label held by a self apparatus, or a label calculable on the basis of a node-corresponding value NV as an intermediate label, and node-added variables salt held by the self apparatus, from the cipher texts;

a label calculating means for calculating a label corresponding to a special subset by executing computational processing based on the node-corresponding value NV and the node-added variables salt, if the subset key to be applied to the cipher text is underivable by the pseudo-random number generating processing based on the label held;

a means for generating the subset key by the pseudo-random number generating processing based on the label held or the label calculated; and

a decrypting means for executing processing for decrypting the cipher text by applying the generated subset key, and

wherein the label calculating means is configured to execute processing for calculating node-corresponding values in a path from a self node to a root being a highest-rank node, among node-corresponding values NV_l (l = 2, 3, ⋯, 2N-1) for respective nodes l to which node numbers l are given from a higher-rank node in a breadth first order in a binary tree, on the basis of the node-corresponding value NV and the node-added variables salt held by the self apparatus, by applying the following expression

[Math 18]

$$NV_{\lfloor l/2 \rfloor} = (NV_{l}^{2} \oplus H^{salt_{l}}(l)) \bmod M$$

where H is a function for mapping an input of any size into a size |M| of a product M of the said two large primes, and H^{saltl} (l) represents a value obtained by applying the function H to l as many as $salt_l$ times.

33. A computer program for generating a hierarchical tree which is applied to processing for supplying cipher texts decryptable only by certain selected equipment except excluded (revoked) equipment, by applying a Broadcast Encryption scheme based on a hierarchical tree configuration, the computer program characterized by comprising:

a one-way tree generating step of generating a one-way tree in which node-corresponding values are set to respective nodes, the node-corresponding values being set such that a node-corresponding value NV_a corresponding to each of the nodes constituting the hierarchical tree is calculable by application of a function f based on a node-corresponding value NV_b and a node-added variable $salt_b$ set so as to correspond to at least one lower-rank node;

a node key calculating step of calculating node keys NK corresponding to the respective nodes constituting the one-way tree, by application of a function Hc using the node-corresponding values NV corresponding to the respective nodes as inputs; and

an information-for-supply determining step of selecting a minimum node-corresponding value and node-added variables required to calculate node-corresponding values included in a path from a receiver-corresponding node to a root as a highest-rank node, as information to be supplied to a receiver corresponding to a terminal node of the one-way tree.

34. A computer program for executing processing for decrypting cipher texts encrypted with node keys respectively corresponding to nodes constituting a hierarchical tree, by applying a Broadcast Encryption scheme based on a hierarchical tree configuration, the computer program characterized by comprising:

a cipher text selecting step of selecting a cipher text to which a node key generable on the basis of node-corresponding values NV and node-added variables salt held by a self apparatus, from the cipher texts;

a node key calculating step of calculating a node key applied to the cipher text on the basis of the node-corresponding values NV and node-added variables salt held by the self apparatus; and

a decrypting step of executing processing for decrypting the cipher text on the basis of the calculated node key.